DETAILED ACTION

This Examiner Amendment and Reasons for Allowance action is in response to the filing of 07/02/2008.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kenneth W. Fields on 09/10/2008.

The application has been amended as follows:

- Claim 1
    - Line 3, insert --stored in memory-- after "secrecy"
    - Line 33 replace "when" with --if--
- Claim 3
    - After line 3 insert --a memory storing a seed value, a verification value, a first encryption information, a second encryption information, a first decryption verification value, a second decryption verification value, a decryption seed value, a decryption shared-key;--

- Line 4 replace "a seed value" with --the seed value--
- Line 5 replace "a verification value" with --the verification value--
- Line 8 replace "first encryption information" with --the first encryption information--
- Line 10 replace "second encryption information" with --the second encryption information--
- Line 15 replace "a first decryption verification value" with --the first decryption verification value--
- Lines 16-17 replace "a decryption seed value" with --the decryption seed value--
- Line 17 replace "a second decryption verification value" with --the second decryption verification value--
- Lines 17-18 replace "a decryption shared-key" with --the decryption shared-key--
- Line 22 replace "when" with --if--

- Claim 24
  - Line 2 insert --and stores in memory-- after "receives"
  - Line 26 replace "when" with --if--
- Claim 46 line 22 replace "when" with --if--
- Claim 47 lines 23 replace "when" with --if--
- Claim 49 line 25 replace "when" with --if--
- Claim 50 line 26 replace "when" with --if--
- Claim 53 line 4 replace "when" with --if--

Allowance

2. Claims 48 & 51 have been cancelled.

3. Claims 1, 3, 24, 46, 47, 49, & 50 have been amended with written arguments which overcome the examiner's prior rejections and objections, see paper of 07/02/08. Examiner withdraws all outstanding rejections and objections to Claims 1-47, 49, 50, 52, & 53.

4. Claims 1-47, 49, 50, 52, & 53 are allowed.

Examiner's Statement of Reasons for Allowance

Prior art was found which disclosed a" two phase cryptographic key recovery system" and "verifiably providing key recovery in a cryptographic system" and "public key cryptosystem (NTRU based)" [i.e. Gennaro et al. (US-5937066-A), Gennaro et al. (US-5907618-A), Hoffstein et al. (WO-9808323-A1)].

5. The following is an examiner's statement of reasons for allowance:

- The prior art of record do not teach or render obvious the limitations as recited in independent Claims 1, 3, 24, 46, 47, 49, & 50, specific to the steps and parts involved in the shared-key generation, usage of a seed value, usage of a verification value, a first and second encryption information each uniquely derived from a verification value and from a verification value based on a seed value, the decryption procedures, the judging based on a verification value to determine outputting of the shared key, etc.
- Therefore, to be more specific, the examiner considers at least the combination of the current limitations and their functionality of shared-key generation and recovery as well as their combinations as claimed comprising, "a seed-value generating unit configured to

generate a seed value" and "a first shared-key generating unit configured to generate a verification value and a shared key, from the seed value" and "a first encryption unit configured to encrypt the verification value to generate first encryption information" and "a second encryption unit configured to encrypt the seed value based on the verification value, to generate second encryption information" and "a transmitting unit configured to transmit to the shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key" and "wherein the shared-key recovery apparatus includes: a receiving unit configured to receive from the shared-key generation apparatus the first encryption information and the second encryption information" and "wherein the shared-key recovery apparatus include: a first decryption unit configured to decrypt the first encryption information, to generate a first decryption verification value" and "wherein the shared-key recovery apparatus include: a second decryption unit configured to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value" and "wherein the shared-key recovery apparatus include: a second shared-key generating unit configured to generate a second decryption verification value and a decryption shared key, from the decryption seed value according to the same method as used in the first shared-key generating unit of the shared-key generation apparatus" and "wherein the shared-key recovery apparatus include: a judging unit configured to judge whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption

seed value being generated based on the received second encryption information and the first decryption verification value, and to judge that the decryption shared-key is identical to the shared-key generated in the shared-key generation apparatus if it is judged that the first decryption verification value is identical to the second decryption verification value" and "wherein the shared-key generation apparatus is distinct from the shared-key recovery apparatus" and "wherein the first encryption information is distinct from the second encryption information," as the non-obvious novelties of the invention;

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
09/10/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436